Chairman Jon Kyl
Opening Statement

Hearing – Wednesday, 12 July 2000

"Identity Theft: How to Protect and Restore Your Good Name"

Senate Judiciary Subcommittee on Technology, Terrorism, and Government Information

Introduction

As chairman of the Subcommittee on Technology, Terrorism, and Government Information, I have always placed a high priority on preventing criminals from using technology to prey upon society.

There are few clearer violations of personal privacy than having your identity stolen and used to commit a crime. Criminals often use Social Security numbers and other personal information to assume the identity of law-abiding citizens and take their money. It's high-tech theft.

Identity Theft and Assumption Deterrence Act

To combat this, I sponsored the Identity Theft and Assumption Deterrence Act,[1] which prohibits stealing a person's identity. The aim of the act, which is now law, is to protect consumers and safeguard people's privacy. Almost two years after passage of the

[1]Pub. L. No. 105-318, October 30, 1998

Act, Identity theft unfortunately continues to grow as the Internet gains in popularity. Teachers, housewives, doctors, and yes even U.S.Senators have been recent victims of identity theft. How does it happen?

. The phone rings and a collection agency demand that you pay a past-due bill for merchandise you never ordered. The supermarket refuses your checks because you now have a history of bouncing them. But you have a perfect credit record, or so you thought, and always paid your bills on time

What happened?

Technology enables new, sophisticated means of identity theft. Using a variety of methods, criminals steal Social Security numbers, credit card numbers, drivers' license numbers, ATM cards, telephone calling cards and other key pieces of a citizen's identity.Some criminals get this information the old-fashioned way: they steal from you're

mail box or your wallet or purse. They may steal your garbage bags, or "dumpster dive" for trash with credit card numbers on them. Your fellow employees may access information from your personnel files. Waiters at restaurants may write down or copy you credit card numbers as you pay for your meal. Attendants at gas stations may double swipe payment cards and sell the data to thieves who specialize in running up the maximum allowance on the stolen credit cards.

Victims are often left with a bad credit report and must spend months and even

years regaining their financial wholeness. In the meantime, they have difficulty writing checks, obtaining loans, renting apartments, getting their children financial aid for college, and even getting hired. Victims of identity theft need help as they attempt to untangle the web of deception that has allowed another individual to impersonate them. Discussions on preventing identity theft often address steps consumers can take, such as shredding their trash and restricting access to their Social Security number (SSN). But realistically, while such measures can decrease the odds of becoming a victim, often there is very little consumers can do to prevent identity theft.

The key to prevention is businesses establishing responsible information-handling practices, and for the credit industry to adopt stricter application-verification procedures and to put limits on data disclosure.

One provision in a bill Senator Feinstein and I proposed would require a credit card issuer to confirm any change of address with the cardholder within 10 days. This will prevent the common method of identity fraud where a criminal steals an individual's credit card number, and then obtains a duplicate card by informing the credit card issuer of a change of address. Credit bureaus would be required to disclose to credit issuers that an address on the application does not match the address on the credit report. Another provision of this legislation would 1) ensure that conspicuous "Fraud Alerts" would appear on credit reports and 2) impose penalties for the

noncompliance by credit

issuers and credit bureaus. Another provision would require the credit issuers and credit bureaus to develop a universally recognized form for reporting identity fraud. Victims could then fill out one form and one affidavit to supply to the numerous companies and entities involved in reporting an identity theft.

These legislative changes and your willingness to adapt best business practices will help victims to

detect errors on their credit history, report the errors efficiently, and help the

victims of identity theft to act swiftly to recover their good name.

Violations of the Identity Theft Act are investigated by federal law enforcement agencies, including the U.S. Secret Service, the FBI, the U.S. Postal Inspection Service and Social Security Administration's Office of the Inspector General. Federal identity theft cases are prosecuted by the U.S. Department of Justice.

Under the law, the Federal Trade Commission collects complaints about identity theft from consumers who have been victimized. The Commission helps victims of identity theft by providing information to assist them in resolving the financial and other problems that can result from this crime.

Statistics

The Office of the Inspector General of the Social Security Administration recently

released a report showing, 81.5 percent of the Social Security Number misuse allegations related to identity theft.[2]

The report reaches the following conclusion:

> Identity theft affects many areas of our society. Private citizens have had their credit histories destroyed by individuals who steal and use their Social Security Number to obtain credit. These individuals run up large credit debts and then move on without paying on the debt. This type of behavior not only destroys the citizen's credit history, it adversely affects the national economy as creditors raise interest rates to cover the losses arising from this fraudulent activity.[3]

Identity theft can, as this report shows, can have a devastating effect.

· In fiscal year 1999 the Social Security Administration Office of Inspector General's hotline for fraud and abuse reported more than 62,000 instances of misuse of Social Security numbers.

· Since November 1999, the FTC hotline and website have logged more than 20,000 calls and 1,500 email complaints regarding identity theft. Some fifty-four percent of the consumers reported that either a fraudulent credit card account was opened in their

[2]Office of the Inspector General, Social Security Administration, Management Advisory Report, A-15-99-92019, at 8 (August 1999).

[3]Id.

name or that there was a fraudulent take over of their existing credit card account. Approximately twenty six percent reported to the FTC that the identity thief opened up telephone, cellular, or other utility service in their name. Approximately sixteen percent reported that a checking or savings account had been opened in their name, and/or that fraudulent checks had been written from their account. Approximately eleven percent reported that the identity theft obtained a loan, such as a car loan, in their name.

Witnesses

Today, the Subcommittee will hear from five witnesses about the effect of Identity Theft and the help that victims of identity theft can expect.

First Panel

- **Jodie Bernstein**, the current Director of the Bureau of Consumer Protection of the Federal Trade Commission(FTC), will discuss how the FTC has responded to identity theft in carrying out its duties under the 1998 law. With the rise of the Internet, personal information about people can often be retrieved with the touch of a keystroke. Director Bernstein will discuss what legislative and non-legislative measures have been taken and what could reduce criminals' access to this sensitive data.
- **James G. Huse**, the current Inspector General of the Social Security Administration, is our next witness. He will discuss how Social Security numbers are used in the commission of identity theft, what steps can be

taken to reduce the role of Social Security numbers in identity theft, why Social Security numbers can be purchased on the Internet for as little as $40, current undercover operations to prevent the sale of Social Security numbers on the internet and what is the most common source of Social Security numbers used for identity theft.

On the Second panel

- **Michelle Suzanne Brown** is a victim of identity of theft. She will discuss her case and will share with us the difficult experience trying to recover her good name through endless phone calls and correspondence with various credit bureaus, credit card companies, her landlord and property manager, police departments, the courts and government. She also will discuss her ideas to streamline the victim reporting process and how to recover and protect yourself from further mistaken identity.
- **Beth Givens** of the Privacy Rights Clearinghouse is our next witness. The Clearinghouse has a new report, "Nowhere to Turn," describing common obstacles experienced by identity theft victims, what measures can be taken to reduce criminal access to sensitive personal information, and how to better provide services to identity theft victims.
- **Steve Emmert** the current President of the Individual Reference Services Group (IRSG), and the current director of the information company Lexis/Nexus. The IRSG is composed of 14 leading information

industry companies that provide data to help identify, verify, or locate individuals. President Emmert will testify how the IRSG members limit the transmission of personal information to prevent criminal misuse. He will testify on the progress of self-regulatory efforts, statistics on enforcement, compliance, and monitoring of member groups.

- And finally, **Stuart Pratt,** Executive Vice President of Government Relations for the Associated Credit Bureaus (ACB), will describe the use of fraud alerts within the credit bureau industry, addressing the duration of the alert, and how credit issuers use alerts. Mr. Pratt will testify about the resources the Associated Credit Bureau has for identity theft victims and its plans to work with credit issuers to streamline reporting of identity theft.

Thank you all for coming.

Closing

In closing, I would like to thank Senator Feinstein for her support in helping the Identity Theft bill to become law. It has been a pleasure to work with her on the Subcommittee initiatives that aim to ensure that the law keeps pace with technology.